UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

CHAIRMAN

March 4, 2002

The Honorable Edward J. Markey
United States House of Representatives
Washington, D.C. 20515-2107

Dear Congressman Markey:

I am responding on behalf of the U.S. Nuclear Regulatory Commission (NRC) to your letters of November 15, 19, and 27, 2001, regarding actions taken by the NRC and the nuclear industry in response to the terrorist attacks of September 11, 2001.

Your letter of November 27, 2001, states that it appears that the NRC downplayed the risk of a terrorist attack on a nuclear reactor and the potential consequences of such an attack in the period after September 11. Your letter referenced statements made by the NRC and a study conducted by Argonne National Laboratory. In the aftermath of the September 11 attack, staff was asked a number of questions and sought to provide immediate responses. The NRC's statements reflected a sincere attempt to be responsive.

During the initial response to the events of September 11, 2001, our intent was to provide the best available information to a wide range of questions and concerns. The subsequent responses to similar questions may have caused confusion when they noted that past NRC reviews had not specifically contemplated attacks by aircraft such as a Boeing 757 or 767, and that nuclear plants were not designed to withstand such crashes. The statement that "detailed engineering analyses of a large airliner crash have not yet been performed" was in the context of situations similar to those of September 11. The 1982 study written for the NRC by Argonne National Laboratory (ANL), and others conducted during that time frame, did not consider attacks or deliberate acts using aircraft, as opposed to airplane accidents, nor did they consider aircraft as large as the Boeing 757 or 767.

The questions you raised in the three letters are very wide-ranging. As a result, rather than summarize the responses here, I refer you to the enclosures for detailed responses to each of your questions. Responses to questions you raised in your letter of December 4, 2001, will be provided in separate correspondence.

As you know, the NRC is conducting a thorough re-evaluation of its security requirements and programs. This re-evaluation will include the control of information that could potentially assist individuals who may attempt to sabotage a licensed facility. Although the staff's re-evaluation is not yet complete, we have responded to your questions with information that is deemed to be sensitive information. Responses that do not contain sensitive information

are provided in Enclosure 1; responses with potentially sensitive information are provided in Enclosure 2, with markings indicating that the information is not for public disclosure. Accordingly, these pages should not be made publicly available.

If you have further comments or questions, please feel free to contact me.

Sincerely,

Richard A. Meserve

Enclosures:
Enclosure 1: Responses to Questions (non-sensitive information)
Enclosure 2: Responses to Questions (sensitive information)

Questions on the NRC's Immediate Response to the Events of September 11

Question 2: In [Chairman Meserve's] October 16th letter, you advised me that the Commission had decided to issue a Threat Advisory on September 11th rather than an order because issuing an order "would have consumed time and resources and would have been no more effective in achieving the desired result."

Question 2.a. Please explain why issuance of an order would have been more time and resources consuming.

Answer:

The Threat Advisory process was put into place with our licensees, prior to September 11, to ensure rapid communication and responses to potential security concerns. As such, it is an understood means of promptly communicating information to licensees to provide guidance when rapid actions are required. Under the circumstances arising on September 11 and thereafter, it was the appropriate regulatory vehicle to accomplish the objective quickly. Subsequent inspections and audits have confirmed appropriate implementation by licensees. If there had been a need to take additional regulatory action, the Commission would not have hesitated to issue immediately effective orders directing the necessary actions.

Question 2.b. Does the Commission believe that any changes in its procedures for issuing orders may be needed in order to assure that such orders can be issued rapidly to respond to emergency situations?

Answer:

The Commission does not believe that any changes are necessary. Such orders can be issued where necessary and appropriate to the circumstances. When warranted, orders can be issued promptly to address emergent situations using current Commission regulations and procedures.

Question 2.c. From a legal and enforcement standpoint, what is the difference between a Threat Advisory and an Order? In your response, please address the consequences of noncompliance by a licensee. Can licensees be fined or otherwise penalized if they fail to implement the heightened security measures asked for in an advisory? If not, wouldn't issuance of an order be more appropriate, in order to signal to licensees that full compliance is expected?

Answer:

An order imposes legally binding requirements upon a licensee and, in accordance with the Administrative Procedure Act, as well as the Atomic Energy Act of 1954, as amended, and the Commission's regulations, requires that the person affected be afforded the right to request a hearing. If a licensee does not comply with the requirements of an order, civil penalties or additional sanctions for such noncompliance may be imposed by further order. Willful noncompliance with an order may result in criminal sanctions, pursuant to Section 223 of the Atomic Energy Act.

By contrast, a Threat Advisory is a guidance document that is not, in itself, legally binding. Nonetheless, if a licensee fails to implement the heightened security measures suggested in an advisory, the Commission may, on a case-by-case basis, issue an order requiring the licensee to perform actions specified in a Threat Advisory based on a determination that the actions are necessary for adequate protection of health and safety and the common defense and security. NRC followup inspections, audits and other communications indicate that licensees have implemented actions in the advisories without the need for further action on the part of the Commission.

Question 3: On September 28, 2001, you sent a memo to the NRC's Executive Director for Operations directing the NRC staff to undertake a comprehensive reassessment of the Commission's security requirements. Please report on what specific actions have been proposed or undertaken in response to that request.

Answer:

In the aftermath of the terrorist attacks of September 11, 2001, and the continuing uncertainty about future terrorist intentions, the Chairman, with the full support of the Commission, directed the staff to undertake a thorough review of its safeguards and security programs. Subsequently, the NRC Executive Director for Operations established the Response to Terrorist Activities (RTA) Task Force comprised of deputy office directors and a deputy regional administrator to conduct this review.

The Commission is currently considering several policy issues identified by the RTA Task Force including: (1) the boundary between private and government responsibility for defending against assumed threats, (2) the NRC's role and interface in national critical infrastructure protection, (3) the approach for balancing national security interests with public information needs, and (4) the NRC's responsibility regarding the consequence of terrorist attacks at licensed facilities that have a potentially significant chemical hazards.

Question 4: In your October 16th letter, you indicated that "all relevant licensees" have implemented a heightened security posture and that "all relevant licensees" remain at an elevated security posture. Please inform me what the Commission means by "relevant licensees." Does this term include all production and utilization facilities, including research reactors and decommissioned reactors and all materials licensees, or are some excluded? If so, please explain the rationale underlying the Commission's decision to include certain licensees, but not others.

Answer:

The advisories that have been issued by the NRC since September 11, 2001, have been sent to various categories of licensees depending on the content of the advisory, the nature of the threat at the time, and the need for each category of licensee to take action, with due consideration being given to limiting information to categories of licensees who need that information to take action. For example, the advisories issued on September 11 and 12 were distributed to power reactors, non-power reactors, category I fuel facilities and gaseous diffusion plants. The advisories sent on September 14 and 21, 2001 were distributed to the same categories of licensees as before, but also to decommissioning reactors and independent spent fuel storage installations. A later advisory was sent to large materials licensees and Agreement States, and one was sent to category 3 fuel facilities and conversion facilities. On October 6, 2001, the NRC issued three advisories outlining specific prompt and additional actions to be taken by licensees. These advisories were distributed to power reactors, non-power reactors, category 1 fuel facilities, decommissioning reactors, independent spent fuel storage installations, and gaseous diffusion plants. Licensees excluded from these advisories were materials licensees possessing small quantities of nuclear materials, such as medical facilities and university research laboratories. However, on October 16, 2001, an advisory was sent specifically to materials licensees to advise them of steps to take to maintain the security of their sites.

While the advisories described above are not the only ones issued, they illustrate the point that not all advisories are appropriate for all categories of licensees, taking into consideration the content of the advisory, the nature of the threat, and the need for each category of licensee to take action.

Question 5: In your October 16, 2001 letter, you indicated that "The NRC has routinely monitored the threat environment since the creation of the design basis threat (DBT) statements in the late 1970s." How many times has the DBT been changed since the first DBT rule was enacted? What specific changes were made in the DBT on each of these occasions, and how did these changes differ in the final rule from those originally put forward in the proposed rule?

Answer:

Each of the design basis threat (DBT) statements used to design physical protection systems has been changed once. The DBT for theft of strategic special nuclear material (SSNM) was modified in 1987 to include the use of a vehicle for transporting personnel and equipment. This change was made in order to maintain comparability with the Department of Energy's threat guidance regarding protection of SSNM. The design basis threat statement for radiological sabotage was modified in 1994 to include: 1) use of a vehicle by an adversary to transport personnel and equipment, and 2) the use of a vehicle bomb. These changes to the DBT of radiological sabotage were made through a notice and comment rulemaking in response to two events that occurred in February 1993. In that month, a vehicle intrusion occurred at the Three Mile Island nuclear power plant and the World Trade Center was bombed. There were no significant differences between the proposed changes and the final design basis vehicle threats.

While each of the DBT statements have only been changed once, the NRC works with federal law enforcement and intelligence agencies to ensure that the DBT remains valid and realistic as compared to the current threat environment. Based on this continuous review, adversary characteristics have been modified to reflect the intelligence information regarding the weapons and tactics that are being utilized by terrorists. These changes are within the general description of the DBT and are provided to the licensees as safeguards guidance.

Question 6: I have received your November 13, 2001 letter regarding the temporary shutdown of the NRC website, and appreciate your updating me regarding the current status of efforts to review materials that had been posted on the site, as well as you consideration of the concerns raised in that letter. As I indicated in my letter of October 15th, I would like a list of all materials removed from the website since September 11, 2001, and an explanation of the basis for the removal of such materials. Please provide such a list as soon as the NRC staff completes its review of the website.

Answer:

Substantial portions of the website have now been restored. We will provide you with a list of the categories or types of documents that are not being restored to the NRC's website once the web review is complete. We will also provide you with a rationale as to why these particular categories of documents will not be restored.

Question 7: On September 12, 2001, in a document entitled "NRC Staff Responses to Contentions Submitted by Donald Moniak et al" in the NRC docket number 070-03909, the Duke Cogema Stone & Webster MOX Fuel Fabrication Facility Construction Authorization Request, NRC stated that "GANE [petitioners] provides no support for its general assertion that `malevolent acts must be analyzed as a foreseeable environmental impact under NEPA . . .and GANE does not establish that terrorist acts (involving the proposed MOX Facility or related materials) fall within the realm of `reasonably foreseeable' events." Does the NRC intend to amend this filing, in light of the events of September 11? If not, why not?

Answer:

As this question notes, the statement is contained in a document entitled "NRC Staff Responses to Contentions Submitted by Donald Moniak . . ." which was filed in the MOX Fuel Fabrication Facility licensing proceeding on September 12, 2001. On December 6, 2001, the Atomic Safety and Licensing Board presiding in the MOX proceeding issued its decision ruling on, among other things, the contentions advanced by the petitioners. The Board admitted the contention in question notwithstanding the staff's position. This matter is subject to further litigation and, ultimately, review by the Commission. Thus, it would not be appropriate for the Commission to comment further at this time.

Questions on Background Checks Required by Employees of Nuclear Facilities

Question 1: Your October 16 letter stated that the background checks required for personnel at nuclear facilities is limited to a check of criminal history, psychological history, training/education, and other behavioral observations. However, you apparently do not require that the background of the individual be checked to ensure that he or she is not a member of a domestic or foreign group that seeks to do harm to the U.S. Do you plan to require this sort of security background check of all current and future employees, in light of the events of September 11? If not, why not, given the possibility that Al Queda [sic] or other groups could seek to place one of their U.S.-based members at a job inside a nuclear reactor to assist as an insider in future terrorist attack on the facility?

Answer:

Licensees process and screen applicants as required by the Commission's regulations, specifically, 10 CFR § 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants," and 10 CFR § 73.57(b), "Requirements for Criminal History Checks of Individuals Granted Unescorted Access to Nuclear Facility or Access to Safeguards Information." These regulations require licensees to establish and implement an access authorization program for granting unescorted access to protected and vital areas of a nuclear power plant. The program objective is to provide high assurance that individuals granted unescorted access are trustworthy and reliable and do not constitute an unreasonable risk to public heath and safety. As part of this access authorization program, licensees fingerprint employees and submit the fingerprint cards to the FBI for a criminal history check on the employee.

A criminal history check of the FBI's National Crime Information Center (NCIC) is conducted using the applicant's fingerprint card submitted by the licensee. NCIC is a nationwide information system dedicated to serving and supporting criminal justice agencies -- local, state, and federal. The check includes the following attributes: felonies, misdemeanors, misdemeanor crimes of domestic violence, other (multiple DUIs, non-NCIC warrants, flash notices, etc), drug abuse, domestic violence restraining orders, fugitive from justice, illegal/unlawful aliens, dishonorable discharges, convicted sex offender registry, denied persons file, and mental defective. The FBI's Integrated Automatic Fingerprint Identification System (IAFIS), a relatively new digital system, will store and search the NCIC database and will compare the prints to all fingerprint data on file.

The criminal history checks conducted by the FBI and associated background checks conducted by licensees ensure that the individual seeking employment does not possess any of the attributes listed above. However, the search is limited to the United States. In other words, US citizens are currently accounted for better than foreign applicants due to the lack of information (e.g.,credit history and criminal history) or unwillingness of the country to provide such information. Licensees determine access to the facility regarding foreign applicants on a "best effort" basis and the applicants are screened and processed as any other individual according to federal requirements.

As a result of the terrorist attacks of September 11, 2001, the Chairman directed the staff to thoroughly reevaluate the NRC's safeguards and physical security programs. This reevaluation

is a top-to-bottom analysis involving all aspects of the Agency's safeguards and physical security programs. This effort includes an examination of the basic assumptions underlying the current program, including access authorization requirements and programs.

Question 2: Your letter also indicates that since September 11th, the FBI has provided the NRC with frequently updated lists of individuals who may have ties or information related to terrorist activities and that, to date, all potential matches have been resolved through the FBI. Were there any positive matches? How many and at what plants? What action was taken?

Answer:

The NRC, its licensees, and the Nuclear Energy Institute participated in multiple reviews of the FBI's Watch List. Although there were some names present on the FBI watch list that were similar to names of individuals who have worked at nuclear facilities, further review of the personal information disproved the match. As a result, NRC in consultation with the FBI determined that there were no positive matches between access authorization lists at the nuclear facilities and the FBI's list.

Question 3: Your letter also indicated that "employees at nuclear power plants do not have to be permanent residents or citizens of the United States." How many of those currently employed at the plants are foreign nationals? What countries are they from? How does the NRC assure that such individuals are properly screened to assure that they do not pose a risk to the security of the facilities due to any associations with any terrorist organizations?

Answer:

According to the regulations in 10 CFR 73.55, there is no requirement that NRC licensees deny employment and/or unescorted access authorization on the basis of an applicant's country of origin. The Commission, therefore, does not have data on the number of foreign nationals employed at nuclear power plants. While records would exist at each power reactor facility concerning the country of origin for all of its employees, the NRC does not maintain copies of that information. The screening requirements do not require the applicants to declare any affiliation with terrorist organizations, although the background investigation, including criminal history, may uncover information that may lead to discovery of such affiliation. See response to Question 1 on page 9.

As part of its broad, top-to-bottom review of physical security requirements, the NRC will consider whether changes are necessary in its access authorization program and requirements.

Questions on the Adequacy of Security Forces at Nuclear Facilities

Question 1: It has been suggested to me that over the last decade, some NRC licensees have significantly reduced their expenditures on security, as well as the number of security personnel at their facilities, resulting in a weakening of security at these facilities. Please provide me with a table listing the total annual security expenditures for each commercial nuclear power plant regulated by the Commission for each of the last 10 years, and the total number of armed security employees employed at such facility during each of the last ten years with responsibilities to respond to attacks. In this table, also provide a column indicating the percentage increase or decrease in security expenditures and numbers of security personnel at each facility during this ten-year period.

Answer:

In accordance with 10 CFR 50.54(p), licensees may make changes to their security programs without prior NRC approval if those changes do not reduce the effectiveness of the security program. Consistent with that regulation, some licensees have installed new technologies for access control, e.g., biometric systems like hand geometry for access control, and were able to reduce the number of guards on shift previously assigned to that function. Reductions in guard strength that are not otherwise compensated must be approved by the NRC before implementation. Normally, such a change would be permitted only when the licensee has demonstrated that its original security plan committed to more guards than would be necessary to protect the site and that the licensee can protect the site with the lesser number.

The NRC does not require licensees to submit information concerning security expenditures. The NRC also does not have information on the number of security personnel at each facility over the last ten years.

Question 2: Is there any variation in the numbers of armed security employees deployed at each plant during periods of "heightened alert," such as those that have followed the events of September 11th? If not, why not, since presumably a period of heightened alert would necessitate an increased number of armed responders?

Answer:

Following NRC's issuance of the advisories in September and October 2001, nuclear power reactor and certain other licensees increased the number of guards and armed responders protecting the plants. The number of security employees varies in accordance with a number of factors, including site design, geography, and response strategies.

Question 3: Does the Commission believe the numbers of persons employed by licensees to protect the plants is adequate in light of the number of terrorists involved in the September 11th attacks, and the potential for similar numbers of terrorists to be involved in a future attack against a nuclear power plant?

Answer:

The NRC has conducted various audits of the licensees' capability to respond to terrorist attacks with the capabilities of the current design basis threat (DBT) and has concluded that the licensee security programs are adequate at this time. The NRC staff is conducting a thorough reevaluation of its safeguards programs, including regulations and the implementation of those regulations by the licensees. This review includes assessment of the current threat environment. From the results of this review, the NRC will propose changes to its regulations and the DBTs, as appropriate, and changes in the way in which licensees protect the nuclear facilities. In the review, we will reevaluate the capability of the licensees' security programs to respond to terrorist attacks consistent with the revised DBTs.

Question 4: Which plant or plants currently deploys the most armed responders? Which plant or plants currently deploys the fewest armed responders? What security rationale justifies these differences, if any?

Answer:

Nuclear power plants differ in the size of the protected areas, the land (and marine) area to which the plant is exposed, the availability of natural cover to be integrated into the protection strategy, the configuration of assets within the protected area, the redundancies built into safety-related equipment, limitations in State laws on weaponry available to the security forces, and other factors. Protection of the site, therefore, must be site-specific, taking these and other factors into consideration. Even the licensee's choice of response strategy can affect the number of armed guards and responders necessary to provide satisfactory protection of the facility. Therefore the numbers of armed responders at different sites cannot usefully be compared to each other without reference to other information.

Site specific information regarding the licensees with the most and the fewest armed responders is sensitive Safeguards Information.

Questions on Force-on-Force Operational Safeguards Response Evaluations at Nuclear Facilities

As you know, the Operational Safeguards Readiness Evaluation (OSRE) program began testing nuclear plant security in 1991 with force-on-force exercises. Since that time, the NRC has conducted OSREs at approximately eight plant sites annually. In FY02, the NRC reduced the number of OSREs scheduled down to six, reportedly to free up resources to evaluate the pilot of the industry's Safeguards Performance Assessment (SPA) program. The OSREs provided the NRC with invaluable insights into actual security performance, identifying vulnerabilities and protective strategy faults that could not be otherwise identified and corrected. However, during a public meeting at the NRC on October 10, 2001, NRC employee Alan Madison stated that the next OSRE had been canceled and future OSREs deferred.

Question 1: Why did NRC choose to cancel the next OSRE and defer future OSREs? Don't you believe that the events of September 11th demonstrate the need for additional strengthened OSREs? Doesn't the cancellation of the OSREs mean that security problems are no longer being identified and fixed, leading to an overall reduction in security at nuclear facilities?

Answer:

The NRC decided that conduct of force-on-force exercises in the current elevated threat environment would pose significant safety hazards to the licensees' employees and negatively impact security effectiveness. As for strengthening of the OSREs, the evaluations conducted under the OSRE program, like all of the inspections conducted by region-based security inspectors, are founded on the design basis threat, the regulations, and the licensee's site-specific commitments. As noted above, the NRC is currently reevaluating its safeguards program and requirements and, if that reevaluation results in changes to the design basis threat, these changes will be incorporated into the inspection program and future OSREs.

As for the identification and correction of security weaknesses, the Reactor Oversight Process (ROP) and the inspections conducted pursuant to it were not designed for heightened threat conditions. In light of the abnormal conditions in which we are operating post-September 11, the NRC issued a number of advisories (described at length above) and conducted audits of the licensees' implementation of actions to respond to those advisories. These audits, and the continuing awareness of licensee security maintained by resident inspectors and region-based inspectors gives the NRC confidence that the licensees' security readiness is adequate at this time.

As for force-on-force drills, the NRC intends to reinstate them when it is deemed safe to do so.

Question 2: On September 11, 2001 the NRC placed nuclear facilities on their highest level of security preparedness. Have any of the dozens of OSREs conducted since 1991 been conducted with the nuclear plant at the highest level of security preparedness? If not, how can the NRC be assured that security performance at this level is better than at lower levels of preparedness?

Answer:

No. In OSREs that were conducted between 1991 and early 2000, licensees were allowed to respond to the mock adversary action with the number of guards the licensee expected to have onsite rather than the number required in the approved security plan. This provided some insight on how well the licensees could perform with an augmented security force. However, it prevented the NRC from reaching a conclusion as to how the licensee would respond using only the resources that it had committed to in its security plan. Therefore, the NRC decided in the ROP beginning April 2000 to evaluate performance at the baseline staffing levels by limiting the licensees to responding with the minimum number of guards committed to in the NRC-approved security plan. This improved the representativeness of the findings for such exercises, but eliminated the opportunity to judge the licensees' performance with additional armed responders.

As for assessing the quality of performance at the highest level of security preparedness, the NRC has conducted audits of the overall protective strategy at the sites, including feedback from the resident inspectors and region-based inspectors and have concluded that the orientation of assets and numbers of guards under Security Level 3 is an improvement over the previous level of readiness.

Question 3: Has the Nuclear Energy Institute's (NEI) guidance for the proposed industry-designed SPA pilot program been approved by the NRC? If not, when will such approval be forthcoming? Will there be sufficient time for NRC staff, inspectors and contractors to familiarize themselves with the final guidance before the pilot program commences so the they can assess the program effectively?

Answer:

As previously noted, a thorough review of the NRC's physical security and safeguards programs was initiated shortly after the September 11 attacks. Before September 11, the Commission agreed to a one-year pilot of the Safeguards Performance Assessment (SPA) program. The intent of the SPA pilot was determine if a more performance-based approach, making greater use of licensee resources while permitting more frequent NRC evaluation of force-on-force exercises, could be developed. During the conduct of the SPA pilot, the NRC would continue OSRE inspections at a rate of six peryear, which would be combined with eight NRC-evaluated SPA inspections.

It is important to note that the frequency of NRC-evaluated exercises would increase from once every eight years under the OSRE program to triennially under SPA program. The performance of more frequent periodic drills and exercises under the SPA program could enhance our licensees' capabilities to protect against the design basis threat of radiological sabotage. Thus, the Commission approved a one-year trial of the SPA program, subject to close NRC oversight and evaluation. A final Commission decision regarding the method of conducting force-on-force testing would follow formal evaluation of the pilot program and the continuing OSRE program.

It was not intended that the NRC approve the detailed NEI implementation guidance for the SPA program processes. Rather, the intent is that a consensus be reached between the industry and the NRC on the broad, programmatic aspects of the guidance and the conduct of NRC-evaluated exercises. Some issues remain which will have to be resolved before the SPA pilot is initiated. Before initiation of the pilot, the NRC will train NRC staff, inspectors and contractor personnel. The training goal is to ensure a thorough understanding of SPA guidance, NRC inspection procedures, and the NRC's approach to achieving effective, independent assessment of the SPA program.

Question 4: Under the SPA program, will NRC evaluate the performance of pilot plants during the evaluated exercise and require immediate correction of any identified security vulnerabilities, or will it confine itself to evaluating only how the exercise is conducted and evaluated by the licensee? How will the public have confidence that adequate security will be maintained at these plants during the pilot?

Answer:

While at the plant for an evaluated exercise, the NRC will ensure that prompt, appropriate compensatory action is implemented for vulnerabilities that affect the operational security of the plant. Independent of licensee initiatives, the NRC may observe other deficiencies. These deficiencies will be brought to the licensee's attention for appropriate action.

During the SPA pilot, the NRC will continue baseline inspections of licensee physical security programs. Such NRC oversight, coupled with the NRC's capabilities to conduct reactive inspections and ongoing resident-inspector oversight at power reactors, helps ensure that adequate security will be maintained at licensed facilities.

Question 5: Under the proposed Temporary Instruction for NRC observation of the SPA pilot program, NRC will not be able to participate actively in tabletop drills and will not be able to choose scenarios for force-on-force testing, which is a departure from the current practice under OSRE. Under these restrictions, how will NRC be able to independently assess whether the licensee's evaluated exercises are sufficiently challenging and are aimed at potential weaknesses in protective strategies, rather than known strengths?

Answer:

Prior to conducting table-top drills or force-on-force exercises in the SPA pilot program, the NRC will be thoroughly briefed on the licensee's protective strategy and will conduct extensive tours of the facility. Therefore, during these activities, the NRC will be able to assess the licensee's capabilities and identify potential weaknesses in or challenges to the strategy, as well as the appropriateness of the scenarios used.

It is important to note here that the SPA program is a pilot program, which is intended to provide the NRC insights on the efficacy of this program to assess a licensee's response strategies and its security program. The methodology and conduct of table-top exercises and force-on-force drills will be evaluated at the end of the pilot program.

Question 6: The NRC has stated that it envisions the SPA pilot program will serve as a test bed for concepts that may be incorporated into the revision of 10 CFR §73.55. NRC's proposed revision includes an expansion of performance testing to incorporate plant operating modes other than full power, as well as targets such as spent fuel storage areas. How will NRC ensure that these concepts are tested in the SPA pilot?

Answer:

These issues will be evaluated and incorporated as appropriate into revisions to 10 CFR §73.55. However, the details on testing these issues during the SPA pilot have not yet been finalized. In addition, the NRC has not ruled out the possibility of testing these issues through the OSRE program or some other force-on-force inspection activity.

Question 7: I understand the NRC's position to be that the OSRE program will continue until a new rulemaking is in place that establishes a requirement for performance tests. Such a rulemaking is likely to take several years. Is it your intention to support the OSRE program at the current rate --- 6 per year --- until a new rule is in place?

Answer:

The NRC intends to continue to conduct OSREs, at least six per year, until a specific rule-based exercise requirement is incorporated into 10 CFR 73.55. Since 1991, OSREs have been conducted at a rate of eight per year and, prior to September 11, the Commission had approved the reduction to six OSREs per year in consideration of the anticipated onset of the industry-initiated Safeguards Performance Assessments (SPAs).

As stated in the answer to Question 1, above, all force-on-force evaluations, whether OSRE or SPA, have been suspended during the current high level threat environment. We intend to resume force-on-force exercises as soon as practicable. As part of the current overall review, the staff is considering all aspects of our security program, including the frequency of OSRE and NRC-evaluated SPA force-on-force exercises.

Question 8: In your October 16, 2001 letter you stated that the NRC has not made a decision to terminate the OSRE program yet, but instead planned on evaluating the results of the industry-sponsored SPA program, in which the industry would test its own security measures, before deciding how to proceed. Why should the Congress or the public have any confidence that industry-designed, supervised, and evaluated tests of its own security systems are adequate? In the aftermath of the September 11th attacks, don't you agree that tests of a licensee's security forces should be a federal function, rather than a function delegated to the licensees themselves? If not, why not?

Answer:

The NRC does not agree that the testing of a licensee's security force needs to be the sole function of a federal entity, even in light of the September 11 events. In accordance with the NRC's regulatory requirements, licensees have a responsibility to ensure that their programs are effective in protecting the public health and safety and the common defense and security. The licensees are required to assess or test the adequacy of their regulated activities, including nuclear security. Self-assessment is a critical part of this process and has been tried, tested and proven beneficial in many NRC-regulated activities. Even if the SPA program were to be adopted in the future, the NRC will maintain its capabilities to conduct independent verification of performance as needed.

Question 9: I understand that, as written, the SPA does not permit NRC "observers" to independently assess potential security weaknesses, as in the OSRE. The OSRE permits/requires NRC inspectors to tour the plant, question insiders at great length, conduct analytic tabletop drills. In contrast, the SPA, as designed and written by the nuclear industry, appears to provide a carefully choreographed and rehearsed demonstration of what the particular plant would want to demonstrate.

Question 9.a. Don't you think that there is an inherent conflict-of-interest in asking the nuclear industry to test itself on power plant security?

Answer:

Nuclear power plant security is similar to other licensed activities for which a licensee is required to implement, manage, and initially assess performance. Licensees are responsible for the effectiveness of their programs. Some form of licensee self-testing is necessary to achieve and sustain effective performance. Through independent verification, whether it is the OSRE, SPA, or other program, the NRC is ultimately responsible for determining that licensed activities protect public health and safety and the common defense and security.

Question 9.b. Rather than replace the OSRE program with such a flawed program, wouldn't it be preferable to step up the number of OSRE tests, so that they occurred at least every 2-3 years instead of once every 8 years? If not, why not?

Answer:

The SPA program has not yet even begun, let alone been assessed. Therefore, it is premature to conclude that it is flawed. No decision has been made to replace the OSRE program with SPA. The frequency of future OSREs and SPAs will be reviewed part of the top-to-bottom review of NRC's safeguards program.

Question 10: In the past, the Commission has provided information to me indicating that the nuclear industry's track record in OSREs has not been satisfactory. Is it not true that the NRC has found potential vulnerabilities in OSRE tests of licensees that could lead to core damage or a radioactive release, in 40 - 50% of all OSREs in recent years?

Answer:

A typical OSRE has several components, including table top drills leading to four force-on-force exercises in which the attacking force attempts to exploit any vulnerabilities the NRC security specialists identify in the plant's protective strategy. The attacking force is credited with detailed knowledge of the plant's lay-out, vulnerabilities and security force defense plans. The overall goal of the OSRE is to improve the efficacy of facility security by identification and correction of weaknesses.

In 37 of 81 OSREs conducted between August 1991 and August 2001, the NRC identified weaknesses.[1] For those plants at which a weakness was found, the attacking force was typically able in one of the four exercises to reach a target set and simulate destruction of that equipment. In general, these weaknesses occurred due to deficiencies in the licensee's contingency response plan, in training, or in executing the plan. No one issue dominates the weaknesses found.

It is agency policy for NRC licensees to address identified weaknesses immediately through the implementation of compensatory measures and, where appropriate, permanent corrective actions. The NRC believes that the program has served an important function by contributing to the identification of areas for improvement in the licensees' security programs. The tests are difficult because they are designed to exploit potential vulnerabilities revealed in the table top drills. They do not necessarily reflect the likelihood of success by a less informed attacking force.

---

[1] For the 15 OSREs conducted between April 2000 and August 2001, weaknesses were identified in 9 of 59 exercises or 15 percent of the time. Eighty-five percent of the time the attacking force was defeated.

Question 11: What criteria does the NRC use to determine whether a licensee's armed responders have passed or failed an OSRE test? If a licensee whose armed responders have, in an OSRE test, proven unable to protect the plant against an act of sabotage resulting in a core meltdown or radiological release, is this a failure, or is it possible to pass despite this result?

Answer:

The OSRE program does not conclude whether a licensee has passed or failed OSRE test, but instead has a purpose of identifying and correcting any weaknesses in the licensee's protective strategy. The licensee's performance for a particular exercise scenario is judged a success if the response force effectively protected against the adversary disabling and/or destroying all pieces of equipment and preventing the operator actions in a target set; and the licensee's performance is judged unsuccessful for the scenario if the response force is not able to prevent the adversary from disabling and/or destroying all pieces of equipment/actions in a target set. The inspectors may also note procedural issues related to the conduct of the exercise, e.g., controller preparation and adversary training and conduct.

Historically, the OSRE team based its conclusions concerning weaknesses in the licensees' response strategies on whether the licensees had the capability (1) to respond with a sufficient number of armed personnel, (2) who were appropriately armed, (3) to protected positions, (4) in time to interdict the adversary before the adversary completed its attack. Cases in which a licensee was unable to satisfy one or more of these criteria would indicate that the adversary could cause an act of sabotage resulting in a loss of a complete target set (i.e., the equipment necessary to be protected to prevent core damage).

Recently, during the conduct of the OSRE, observations and findings would be evaluated to identify the risk significance of deficiencies in the licensee's protective strategy and/or the licensee's ability to implement the strategy in accordance with the revised reactor oversight process. While this approach has provided a more understandable and consistent approach to evaluating OSRE results, the four items noted above still form the core evaluation criteria.

Question 12: Please provide a summary of the results of each OSRE test conducted since the inception of this program. This summary should include the following information: Plant tested, security company contracted by the plant at the time of the test, date of test, summary of results of tests (including, but not limited to identification of any security weaknesses identified in the test and the root causes of such weaknesses), and actions taken (if any) by the licensee in response to weakness identified in the test.

Answer:

The answer to this question contains sensitive information, not for public disclosure. Therefore, it has been separated from this enclosure to allow the information in it to be controlled, and not be publicly released.